

Az igazsággépezet

Michael J. Casey–Paul Vigna: *The Truth Machine – The Blockchain and the Future of Everything*
St. Martin's Press, New York, 2018, 302 o.

A kriptovaluták kora című – a jelen kötet előzményének tekinthető – könyvükben a szerzők a kriptovalutákban rejlő lehetőségeket tárták fel, egy igazságosabb globális fizetési rendszer létrehozása érdekében, amelyben nem léteznének bankok vagy pénzügyi közvetítők (Casey–Vigna [2016]). Az igazsággépezet című második kötetük e gondolat kiterjesztése, amely azt vizsgálja, hogy a Bitcoin¹ mögött álló blokklánc- (*blockchain*) technológia hogyan definiálhatja újra nagy általánosságban számos más, új felhasználási területen a társadalmi szerveződéseket és az intézményrendszereket.

A blokklánc az első olyan technológia, amellyel olyan adatbázisokat lehet létrehozni és működtetni, amelyekre bárki ráláthat, amelyek bármikor ellenőrizhetők, de semmilyen központi entitás nem gyakorolhat felettük teljes kontrollt. Ez azt jelenti, hogy senki sem tudja megváltoztatni az ezen adatbázisokban tárolt információkat, viszont mindenkinek biztosabb ellenőrzési lehetősége van a saját adatait illetően. A blokklánc-technológia így egy ősrégi társadalmi problémát orvosol, a bizalom hiányának kérdését, mivel társadalmi tőkét (*social capital*) generál a közösség tagjai között.

A mai napig a társadalmi tőke gondozásában olyan „megbízható harmadik fél” (*trusted third party*) jellegű intézményekre támaszkodunk, mint a bankok vagy a kormányhivatalok. A szerzőpáros szerint probléma, hogy ezek az intézmények egyben kapuórként is funkcionálnak, valamint többletköltségeket jelentenek a gazdasági kapcsolatokban, arról nem is beszélve, hogy szélsőséges esetekben, például válságok idején, akár diszfunkcionálissá is válhatnak. A blokkláncalapú rendszerek alapfogdolása, hogy e problémákat kivédendő, a megbízható harmadik felek helyett közös protokollon alapuló, decentralizált hálózatokba delegáljuk a társadalmi tőke gondozását.

A Bitcoin tervezői egy olyan pénzügyi eszközt kívántak létrehozni, amellyel megkerülhetik a bankokat és kormányokat, amelyek évszázadok óta a pénzügyi rendszerek őrzői. A történelem során az írás, a pénz és a könyvelés hármassága tette lehetővé,

¹ A szerzők a könyvben végig *Bitcoin* elnevezéssel hivatkoznak az azonos nevű kriptovalutára, míg *bitcoin* elnevezéssel magára a rendszerre és protokollra, amely a blokkláncalapú kriptovaluták működését teszi lehetővé.

hogy kis csoportokon túlmutatóan is bonyolódhassanak üzleti kapcsolatok. A pénz önmagában is nyilvántartó eszköz. Az arany és a papírpénz a közösség által elfogadott érték hordozója, amely valamilyen jogot biztosít javakhoz vagy szolgáltatásokhoz, és egyben igazolja a múltban elvégzett feladatokat is.

Ahogy a kereskedelem földrajzilag egyre kiterjedtebbé vált, már főként biztonsági okokból sem volt lehetőség arra, hogy az emberek fizikailag is magukkal vigyék a pénzt. A megoldás a kettős könyvelés formájában jelent meg, amit a reneszánsz kori bankárok terjesztettek el. Ez évszázadokon keresztül segített a gazdasági kapcsolatok fejlesztésében, tulajdonképpen ez vált a modern banki tevékenység alapjává. A könyvelés elterjedése azonban egy újabb dilemmát is felvetett: vajon a társadalom megbízhat-e a könyvelőben?

A bitcoin úgy kívánja orvosolni ezt a problémát, hogy újratervezi a főkönyvet a könyvelő, azaz a megbízható harmadik fél kiiktatásával. Az új főkönyv független számítógépek összességéből áll, ahol a tranzakciók közvetlenül zajlanak le az egyes résztvevők között. A blokklánc tehát nem egy bizalom nélküli rendszert kíván létrehozni, hanem egy olyan eszközt szándékozik nyújtani, amely segít a bizalom és a társadalmi tőke megerősítésében. E konszenzusépítő képessége miatt hivatkozik rá a szerzőpáros mint „igazsággépezetre” (*truth machine*). Szerintük ahhoz, hogy feloldjuk azt a dilemmát, hogy mire vagy milyen intézményekre bízunk az adatainkat, érdemes a centralizálttól egy decentralizált bizalmi modell irányába elmozdulni. Rendkívül nehéz technikai és politikai kihívás azonban egy olyan decentralizált gazdasági rendszer felépítése, amely független, anonim számítógépek hálózatából áll, és amelyben mindenki a köz érdekében cselekszik.

A Bitcoin mellett a leginkább ismert blokkláncalapú platform az Ethereum – egy kanadai születésű, orosz származású programozó, Vitalik Buterin találmánya. Az Ethereum mögötti új elgondolás, hogy nem kizárólag pénz, hanem bármi más, például ingatlanokkal kapcsolatos jogi szerződések, egészségügyi adatok vagy szellemi tulajdonjogok is – okosszerződések révén – gazdát cserélhetnek egy blokkláncalapú hálózaton belül. Ennek az új, univerzálisan hozzáférhető, decentralizált, globális szuperszámítógép-hálózatnak a létrehozása forradalmi elképzelésként tört be. Elképzelhető kezdeti népszerűsége ellenére azonban az Ethereum technológiája egyelőre meglehetősen fejletlen és könnyen támadható.

Az Ethereumhoz hasonló platformokhoz kapcsolódó kriptovaluták (tokenek) névuma többek között abban rejlik, hogy „programozható pénzként” működnek, azaz egy bizonyos kíváncsú magatartásforma irányába tudják terelni a közösség tagjait. A tokenek ily módon segíthetik a közjavak megfelelő kihasználását, azaz a „közlegelők tragédiájának” (*tragedy of the commons*) elkerülését. Egy ideális tokenstratégiában a pénz erkölcsileg nem semleges csereeszköz, hanem magában foglalja a közösség által fontosnak tartott értékeket, valamint azon szereplők érdekeit, akik a tokent használni kívánják. A rendszer lényege, hogy minél többen használják az adott tokent, annál inkább érvényesülnek a pozitív hálózati hatások és viszszaesetelések. Példaként említhető, hogy mivel az Ethereum lett az okosszerződések elsődleges platformja, ez még inkább emelte az ether – az Ethereum-rendszer saját kriptovalutájának – értékét. A jelenlegi probléma a tokenek használatával pontosan

az, hogy a hatalmas piaci kereslet miatt sok esetben olyannyira felülárazottá váltak, hogy ez már arra sarkallja az embereket, hogy felhalmozzák, és ne használják őket, amivel elvész az eredeti funkció.

A szerzőpáros szerint egy likvid, digitális tokeneken alapuló gazdaságban elvben már nem is lenne szükség pénzre, hiszen barteralapon cserélhetnének gazdát javak és szolgáltatások. Akár kocsik, házak vagy olyan immateriális javak is áruba bocsáthatók lennének, mint például a márkák. Ennek egy szélsőséges példája a márkákhoz rendelt hűségpontok cserekereskedelme, amely először a cégek, később a hírességek személyes márkája után akár a mindennapi emberek megbízhatóságára, megbecsültségére is kiterjedhetne, így létrehozva az úgynevezett hírnévtokeneket (*reputation tokens*).

A tokenek használata olyan témákban is felmerült, mint a klímaváltozás megállítása. A Világgazdasági Fórum egyik kezdeményezésében olyan óceán- és klímaérmeket lehet vásárolni, amelyekkel környezetvédő intézkedéseket finanszíroznak. Ha a környezet állapotában mérhető javulás következik be, a kibocsátó szervezet megsemmisíti a tulajdonában lévő tokenek egy részét, hogy így emelje a fennmaradó tokenek értékét. A rendszer mögött álló központi gondolat, hogy bármilyen vagyontöbblet nem feltétlenül nulla összegű játék, azaz lehet önmagát erősítő, innovációt ösztönző és társadalmilag inkluzív folyamat.

A tokenek és kriptovaluták kereskedése mellett a szerzőpáros a blokklánc-technológia számos más megatározó alkalmazási lehetőségére is felhívja a figyelmet. Ilyen az internet potenciális újratervezése olyan formában, hogy az megfeleljen az eredeti decentralizációs elveknek. A szerzőpáros véleménye szerint jelenleg az internetet néhány domináns cég birtokolja (a Google, az Amazon, a Facebook vagy az Apple), s bár a nagyközönség úgy gondolja, hogy ingyenesen használja e cégek szolgáltatásait, valójában cserébe értéket teremt, tartalom és információ formájában.

A *freemium* (ingyenes prémiumszolgáltatás alapú – a *free* és a *premium* szó összevonásából) működési modell így digitális levíttakat teremtett, amelyek példa nélküli monopóliumot élveznek a társadalom legfontosabb adatait illetően. A blokkláncalapú decentralizálás célja lenne megszabadulni a már említett közvetítőktől, hogy az emberek közvetlenül léphessenek interakcióba egymással. Az internet első verziója, az úgynevezett információ internete (*Internet of Information, IoI*) lehetővé tette az adatok átadását. Ezzel szemben a közelgő, úgynevezett értékek internete (*Internet of Value, IoV*) már lehetővé tenné, hogy az emberek értékeket képviselő jogosítványokat osszanak meg egymással az online térben. Ez azt jelenti, hogy bárki egy rendelkezésre álló eszközzel közvetlenül kapcsolódhatna be a világgazdaságba.

Az emberi interakciókon túl a szerzőpáros szerint a blokkláncalapú rendszerek alkalmazása az egyetlen mód arra, hogy úgy építsük fel a dolgok internetét (*Internet of Things, IoT*), hogy egyben biztosítsuk, hogy senki se gyakorolhasson föltte kizárólagos kontrollt. A gazdasági lehetőségek új horizontját tárná fel, ha létre tudna jönni egy olyan blokkláncalapú rendszer, ahol a gépek közötti tranzakciók valóban decentralizált módon zajlanak, és a különböző okoseszközök önállóan tudnak kommunikálni és kereskedni egymás között.

A blokklánc használata emellett a globális értékláncok menedzsmentfolyamataiban is meghatározó lehet. Blokkláncalapú nyilvántartást használva biztosítani

lehetne, hogy adott – például – minőségbiztosítási vagy munkavédelmi folyamatokat elvégezzenek. Egy többszereplős beszállítói hálózatban akár tokenek formájában is kereskedhetnének egymással a felek, valamint a nagyvállalatok közvetlenül hitelezhetnék a kisebb beszállítóikat.

A blokklánc-technológia egy másik fontos felhasználási területe az energiagazdálkodás. Az „energiademokrácia” lényegi gondolata, hogy a környezetterhelést nem kizárólag a káros anyagokat kibocsátó erőművek okozzák, mert ehhez a centralizált hálózati modell is nagyban hozzájárul, mivel jelentős veszteséggel működik. Ezzel szemben mikrohálózatok (*microgrids*) felhasználásával és okosmérőórák segítségével blokkláncalapon kereskedhetnének egymással a felhasználók, kilowattóra-tokenekben. Így optimalizálni lehetne az energiatermelést, a rendszer ellenálló képességét, a veszteségeket pedig minimalizálni.

Egy másik nagy témakör a pénzügyi blokklánc technológiai terén a jegybanki digitális *fiat* valuták kérdése. A szerzőpáros várakozásai szerint alapjaiban fogja megváltoztatni a pénzügyi rendszereket, ha a központi bankok elkezdene kísérletezni a digitális valutákkal. A fogyasztók számára ugyanis biztonságosabb és valószínűleg olcsóbb lenne a jegybankban tartani a pénzüket, mint a kereskedelmi intézményeknél. Így a jegybankok közvetlen versenytársaivá válnának a kereskedelmi bankoknak.

A Bitcoin rendszere – a kriptovaluta-műveleteken túl – az időben való bélyegzés lehetőségét is kínálja, ami lehetővé teszi hivatalos aktusok rögzítését. A Bitcoin 2.0 nevű alkalmazás egy olyan felhasználási metódust indított, amiben a Bitcoin-tranzakciók metaadataiba beillesztenek egy bizonyos azonosítósza-
mát (például egy gépkocsi alvázszámát vagy egy telek helyrajzi számát). Az adat így az algoritmuson keresztül rögzítésre kerül egy olyan Bitcoin-tranzakcióban, amelyben csak egy jelképes összeget utalnak át. Az információ ezáltal, időben bélyegezve, iktatásra kerül a blokkláncban. A valós pénzzel szemben a kriptovaluták tehát programozhatók, azaz hordozhatnak többletinformációt, ami a szerzőpáros várakozásai szerint megnyithatja az utat akár a hivatalos nyilvántartások demokratizálásához is.

Nem olyan régen még a legtöbb személyes adatot számon tartó intézmények a legnagyobb országok kormányai voltak, azaz Kína, India, az Egyesült Államok és Indonézia kormányai. Ma már a top ötben benne van a Facebook, a Google és a Twitter is. Amíg a fejlett világ a túl sok adattal való visszaéléstől tart, a fejlődő világban éppen az ellenkező problémával szembesülnek, azaz túl kevés a rendelkezésre álló személyi adat. A Világbank statisztikái szerint, 2,4 milliárd embernek nincs hivatalos személyazonosságot igazoló dokumentuma, így egyrészt nem férhet hozzá alapvető szolgáltatásokhoz, másrészt kiszolgáltatottá válik a visszaélésekkel szemben. A technológiahívők az államtól való függőség megoldására vetették fel a szuverén személyazonosság koncepcióját, azaz hogy minden ember saját maga kontrollálja az élete során róla összegyűlt adatokat.

Az ilyen digitális identitás létrehozására a szerzők értelmezésében a jelenleg létező legjobb modell a nyilvános kulcsos kriptográfia, amelyet a blokkláncrendszer is alkalmaz. Ez a megoldás lehetővé tenné azt is, hogy ha valakit egy adott intézmény már azonosított, az más intézmények szolgáltatásaihoz is hozzáférhessen, akár egy globális személyazonossági rendszer formájában. Idővel akár hivatalos okiratok is rögzítésre

kerülhetnek majd egy blokkláncalapú kollektív tárolási rendszerben, amire a felhasználók saját személyes kulcsuk megadásával hivatkozhatnak.

A blokklánc-technológiában rejlő lehetőségek iránt tanúsított néhol talán túlzó optimizmus ellenére a szerzőpáros mégis hangsúlyozza, hogy a decentralizáció nem jelent megoldást minden problémára. A társadalom előtt álló kihívások legyőzésére sok esetben akár hatékonyabb eszköz is lehet egy centralizált struktúra, amennyiben jól működnek a közvetítő intézmények. A szerzőpáros a legfontosabb kihívásként jelenleg az internet redecentralizálását jelöli meg. Ez lenne ugyanis a visszatérés az internet eredeti víziójához, amely visszaszorítaná a technológiai óriásvállalatokat, amelyek túlzott befolyásra tettek szert az adatainkat és általánosságban az életünket illetően.

Casey és Vigna meggyőződése, hogy a jövőt három nagy hatalmi központ fogja meghatározni: a technológia, a pénzügyek és a politikai kormányzás. Az Egyesült Államok esetében tehát a Szilícium-völgy, New York és Washington. A legfőbb szembenállás már nem a bal- és a jobboldal, a konzervatív és a liberális, a Nyugat és a Kelet, hanem a centralizált és a decentralizált rendszerek között lesz.

Mindezen új elgondolás megjelenése a szabályozási technológiák rohamos fejlődéséhez is vezet, és az olyan úttörő országok, mint például Észtország, az állampolgári technológiák (*civic technologies*) valós laboratóriumává válnak. A blokkláncfelhasználásokkal foglalkozó *startup* és *fintech* cégek ugyanis a befogadó jogi környezet körül összpontosulnak. Erre jó példa Zug városában a svájci „Kripto-völgy” esete vagy a brit pénzügyi felügyelet szabályozói *sandbox* projektje.

A pénzügyi-gazdasági fejlesztések mellett van egy másik lényeges oldala is a decentralizációnak, amely az állampolgári jogokhoz kötődik. A szerzőpáros várakozásai szerint a blokklánc-technológia révén ugyanis az egyének először lehetnek majd önálló és független szereplői a globális gazdaságnak, valamint a teljes jogú tulajdonosai saját szellemi és tárgyi vagyonuknak. Ezért forradalmi gondolat egy olyan „igazsággépezet” elképzelése, amelyet semmilyen személy vagy intézmény nem tud elpusztítani.

Hivatkozások

CASEY, M.–VIGNA, P. [2016]: *The Age of Cryptocurrency. How Bitcoin and the Blockchain Are Challenging the Global Economic Order*. St. Martin's Press, New York.

Balogh Lilla Sarolta